WHAT IS CLAIMS

1. A method for key management and assignment for information encryption in a radio network system which include a root node, plurality of intermediate nodes in the root node and plurality of leaf nodes in each intermediate nodes of the radio network system providing Multimedia Broadcast or Multicast service, comprising the steps of:

generating a group key for the root node which has plurality of intermediate nodes as child nodes;

generating intermediate key using the group key for each of the intermediate nodes that owns both one parent node and one or more child nodes having its own intermediate key;

requesting a leaf node key in a user equipment (UE) for the service; and

delivering a private key as a leaf node key to the UE on a dedicate channel.

2. The method as defined in Claim 1, wherein each user keeps node key information on all nodes that the node chain where he/she locates to the root node of the tree, including leaf node, intermediate nodes of respective layers and the root node.

3. The method as defined in Claim 1, wherein when a new user joins in the service, this user is connected to a node via its access parent node as a new leaf node and this user needs to obtain keys of all nodes including intermediate nodes and root nodes that are passed by the node chain from the access parent node to the root node; these node keys won't be updated due to the joining of the user; the transmissions of these node key are sent to the user sequentially in point-to-point mode and are encrypted by using the key of the new leaf node.

4. The method as defined in Claim 1, wherein when a new user joins in the service, this user is connected to a node as a new leaf node via its access parent node and this user needs to obtain keys of all nodes including intermediate nodes and root nodes that are passed by the node chain from the

access parent node to the root node; these node keys will be updated due to the joining of the user; for the newly-joined user, the transmissions of these new nodes keys are sent to the user sequentially in point-to-point mode and are encrypted by using the key of the new leaf node.

5. The method as defined in Claim 4, wherein for each node that needs key update, new keys will be encrypted with old keys and will be delivered to the final leaf node's users that they belong to in point-to-multipoint broadcast mode.

6. The method as defined in Claim 1, wherein when a user leaves the service, a leaf node is disconnected from its parent node and the keys of all nodes that the node chain passes by from the disconnected node to the root node of the tree are sequentially updated.

7. The method as defined in Claim 6, wherein for each node that needs key update, the key update of node is performed only after key updates of all its child nodes finish.

8. The method as defined in Claim 6, wherein for each node that needs key update, the new node keys are delivered to all child nodes of it one by one in point-to-point mode and are encrypted with key of each child node.

9. The method as defined in Claim 8, wherein each child node still uses the corresponding node key to encrypt the new node key, and delivers the new node key to the final leaf node's users that they belong to in point-to-multipoint mode.

10. The method as defined in Claim 1, wherein the information encryption process is accomplished by RNC.

11. The method as defined in Claim 1, wherein the root node locates in the same logical network device as that intermediate node does.

12. The method as defined in Claim 1, wherein said root node locates in the different logical network device from that intermediate node does.